IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Ralph Samuel HOEFELMEYER et al.	
Application No.: 09/911,592	Group Art Unit: 2131
Filed: July 24, 2001	Examiner: Chen, S.
Customer No.: 25537 Attorney Docket: COS00019 Client Docket: 09710_1007	

For: NETWORK SECURITY ARCHITECTURE

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated October 26, 2005.

I. REAL PARTY IN INTEREST

Verizon is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

III. STATUS OF THE CLAIMS

Claims 1-15 are pending in this appeal. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-15 on August 15, 2006.

IV. STATUS OF AMENDMENTS

No amendment to the claims has been filed since the final rejection of claims 1-15 on August 15, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent system claim 1.

Independent claim 1 is directed to a network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone. (*See*, e.g., Specification ¶ 4 and FIG. 1) The claimed system comprises a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code. (*See*, *e.g.,* Specification ¶¶ 5, 14, 22 and 25) The claimed system comprises an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets. (*See*, *e.g.,* Specification ¶¶ 5, 27–29 and 30) The claimed system comprises a switch coupled between the internet backbone (*See*, *e.g.,* Specification ¶¶ 5, 15, 16, 19, 20, 33 and 34) the scanning system, and the anti-virus server, said switch configured for directing incoming electronic mail from the internet backbone to the scanning system. (*See*, *e.g.,* Specification ¶¶ 5, 15, 19, 20–26, 32, 36)

Independent system claim 3.

Independent claim 3 is directed to a network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone. (*See*, *e.g.,* Specification ¶ 4 and FIG. 1) The claimed system comprises a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code. (*See*, *e.g.,* Specification ¶¶ 5, 14, 22 and 25) The system comprises a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code (*See*, *e.g.,* Specification ¶¶ 16, 20, 21 and 25) and directing the incoming electronic mail to the scanning system when the incoming electronic mail is determined to be scanned for malicious code. (*See*, *e.g.,* Specification ¶¶ 20 and 25) The claimed system comprises an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets. (*See*, *e.g.,* Specification ¶¶ 5, 27–29 and 30) The system further comprises a switch coupled between the internet backbone, the scanning system (*See*, *e.g.,* Specification ¶¶ 5, 15, 16, 19, 20, 33 and 34), and the anti-virus server, said switch configured for directing incoming electronic mail from the internet backbone to the mail proxy server. (*See*, *e.g.,* Specification ¶¶ 5, 15, 19, 20–26, 32, 36)

Independent system claim 5.

Independent claim 5 is directed to a network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone. (*See*, *e.g.,* Specification ¶ 4 and FIG. 1) The claimed system comprises a plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code. (*See*, *e.g.,* Specification ¶¶ 5, 14, 22 and 25) The system comprises a plurality of anti-virus servers coupled to the intranets for downloading anti-virus code to clients coupled to the intranets. (*See*, *e.g.,*

Specification ¶¶ 5, 14, 16, 19 and 21–23) The system further comprises a plurality of switches coupled between the internet backbone (*See, e.g.,* Specification ¶¶ 5, 15, 16, 19, 20, 33 and 34), the scanning systems, and the anti-virus servers, said switches configured for directing incoming electronic mail to at least one of the scanning systems. (*See, e.g.,* Specification ¶¶ 5, 15, 19, 20–26, 32 and 36)

Independent method claim 8

Independent claim 8 is directed to a method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone. (*See, e.g.,* Specification ¶ 4 and FIG. 1) The claimed method comprises directing incoming electronic mail from the internet backbone to a scanning system. (*See, e.g.,* Specification ¶¶ 05, 15, 20, 25 and 28) The method comprises scanning incoming electronic mail for malicious code. (*See, e.g.,* Specification ¶¶ 16, 20, 21 and 25) The claimed method further comprising downloading anti-virus code to clients coupled to the intranets. (*See, e.g.,* Specification ¶¶ 5, 27–29 and 30)

Independent method claim 10

Independent claim 10 is directed to a method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone. (*See, e.g.,* Specification ¶ 4 and FIG. 1) The claimed method comprises directing incoming electronic mail from the internet backbone to one of a plurality of mail proxy servers at the one of the mail proxy servers. (*See, e.g.,* Specification ¶ 16, 20 and 25) The method comprises

determining whether the incoming electronic mail is to be scanned for malicious code. (*See, e.g.,* Specification ¶¶ 16, 20, 21 and 25) The method comprises directing the incoming electronic mail to a scanning system when the incoming electronic mail is determined to be scanned for malicious code; at the scanning system (*See, e.g.,* Specification ¶¶ 05, 15, 20, 25 and 28), scanning incoming electronic mail for malicious code. (*See, e.g.,* Specification ¶¶ 5, 21, 23, 25 and 26) The method further comprises downloading anti-virus code to clients coupled to the intranets. (*See, e.g.,* Specification ¶¶ 5, 27–29 and 30)

Dependent claims argued separately (claims 2, 4, 7, 9, 6-11 and 12-15)

In addition to the switch, a Denial of Service (DoS) or Distributed DOS scanning/filtering switch may be employed to prevent these specific attacks. In one embodiment, a decoy server is also provided for masquerading as a legitimate server and logging suspicious activity from communications received from the internet backbone. (*See, e.g.,* specification, ¶ 05, claims 2, 4, 7, and 9)

In the architecture illustrated in FIG. 1, one or more front-end switches 110 are coupled to the Internet backbone 100 and provide the basic gate-keeping functionality of the architectures. In one implementation, the front-end switches 110 also measure and record the communications traffic between the customers' systems and the Internet for billing purposes. The front-end switches 110, which may be implemented with one or more CISCO™ 6509 switches, are thus responsible for receiving communications from the Internet backbone 110, directing the Internet communication to an appropriate security server for detecting and responding to incoming threats, and load balancing among the security servers. (*See, e.g.,* specification, ¶ 15, claims 1-

11) Accordingly, the front-end switches 110 are positioned to intercept incoming electronic mail and other communications before they are routed to the customers' systems. The switches are also connected directly to DoS/DdoS scanning/filtering switches operating at line speed. (*See, e.g.,* specification, ¶ 15)

A local area network 120, such as a fast ETHERNET™ network, couples the front-end switches 110 with the security servers, which comprise, for example, one or more mail proxy servers 130, one or more antivirus scanning servers 140, one or more client antivirus servers 150, one or more decoy servers 160, and a quarantine server 170. The front-end switches 110, the mail proxy servers 130, the antivirus scanning servers 140, the client antivirus servers 150, and the decoy servers 160 are in communication with a hub 180, which communicates with client intranets 190 that belong to respective customers. (*See, e.g.,* specification, ¶ 16, claims 1-15)

When the electronic mail message is received by one or more of the antivirus scanning servers 140, the electronic mail message is scanned for malicious code (step 209). In one implementation, antivirus scanning software on the one or more of the antivirus scanning servers 140 employs a catalog of viral signatures, which are often simple strings of bytes that are expected to be found in every instance of a particular virus. Usually, different viruses have different signatures, and the antivirus scanning software use signatures to locate specific viruses. To improve coverage, antivirus scanning software from multiple vendors may be employed, and the scanning may be performed on respective antivirus scanning servers 140 for improved performance. (*See, e.g.,* specification, ¶ 22)

If the electronic mail message is infected, tested at step 211, then the antivirus scanning server 140 may attempt to repair the infected portion of the electronic mail message, e.g. an attachment (step 213), as determined by policy. If the electronic mail message or its attachment cannot be repaired (tested at step 215), then the electronic mail message is quarantined (step 217)

by transferring the original, infected electronic mail message to the quarantine server 170 and by removing the infected portion from the electronic mail message to create a sanitized electronic mail message; this action may be varied by policy. The infected electronic mail message can be analyzed at the quarantine server 170 to study the virus, e.g. to generate a new viral signature or determine a new way to sanitize or repair a file infected with the virus. (*See, e.g.,* specification, ¶ 23, claims 12-15)

In either case, when the electronic mail message is infected, the sender and recipient of the electronic mail message may be notified of the detection of the viral infection (step 219), as determined by policy. This notification may be performed by appending text explaining the viral infection to the body of the electronic mail message or as a new attachment or even by composing and sending a new electronic mail message to the sender and recipient of the infected electronic mail message. (*See, e.g.,* specification, ¶ 24)

When the electronic mail message has been sanitized, by passing the antiviral scan (step 209), being repaired (step 213), or being quarantined (step 217), the sanitized electronic mail message is directed to the recipient, via hub 180 and the appropriate intranet 190. Accordingly, a scalable, resilient server-side antivirus scanning architecture is described, in which preferably multiple mail proxy servers 130 and antivirus scanning servers 140 are deployed to catch and sanitize incoming electronic mail messages. When malicious code is detected, an event is generated to the security management system. (*See, e.g.,* specification, ¶ 25, claims 12-15)

If, on the other hand, the incoming communication is not authorized (tested in step 405), then execution proceeds to step 407 where the incoming communication is routed to one of one or more decoy servers 160. A decoy server 160 is a computer system that is configured to look like the client's computer system. Thus, when the unauthorized communication is routed to the decoy server 160, the decoy server 160 simulates the client's computer system (step 409).

Because the decoy server 160 is separate from the client's computer system, any activity at the decoy server 160 performed by the intruder will not affect the client's computer system. In one aspect, the decoy server 160 also includes some un-patched operating system/application holes to look more appealing or breakable to a would-be intruder.

When the intruder takes the bait of the decoy server 160, all actions and keystrokes of the intruder are logged to the administration console 161 (step 411). Consequently, the intruder's action can be studied to understand the nature of the intrusion and learn how to counter the intrusion or to ascertain the source of the intrusion. In addition, an electronic mail alert can be sent from the administration console 161 to an operator to inform that a penetration attempt is underway. (*See, e.g.,* specification, ¶¶ 32-36, claims 2, 4, 7 and 9)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 3, 5, 8, and 10 are properly provisionally rejected under obviousness-type double patenting over claim 1 of Application Serial No. 10/024,202.

Whether claims 1, 3, 5, 8, and 10 are obvious under 35 U.S.C. § 103 based on *Bates et al.* (US 6,785,732).

Whether claims 2, 4, 7, and 9 are obvious under 35 U.S.C. § 103 based on *Bates et al.* (US 6,785,732) in view of *NAI* (Network Associates, Inc., "Network Associates Ships Cybercop Sting - Industry's First 'Decoy' Server Silently Traces and Tracks Hacker Activity").

Whether claims 6 and 11 are obvious under 35 U.S.C. § 103 based on *Bates et al.* (US 6,785,732) in view of *NAI* (Network Associates, Inc., "Network Associates Ships Cybercop Sting - Industry's First 'Decoy' Server Silently Traces and Tracks Hacker Activity") and *Caccavale* (US 2002/0129277).

Whether claims 12-15 are obvious under 35 U.S.C. § 103 based on *Bates et al.* (US 6,785,732) in view of *NAI* (Network Associates, Inc., "Network Associates Ships Cybercop Sting - Industry's First 'Decoy' Server Silently Traces and Tracks Hacker Activity") and *Kim et al.* (US 6,701,440).

VII. ARGUMENT

A. CLAIMS 1, 3, 5, 8, AND 10 ARE PATENTABLY DISTINCT OVER CLAIM 1 OF CO-PENDING APPLICATION 10/024,202

Whereas instant claim 1 is silent as to any security manager and the taking of any action responsive to detection of a malicious code, claim 1 of Application Serial No. 10/024,202 recites that "in response to detection of an instance of malicious code, generating and transmitting an event indicating the detection to a security manager."

Whereas instant claim 3 recites "a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code...," claim 1 of Application Serial No. 10/024,202 is silent as to any such mail proxy server.

Whereas instant claim 5 recites a "plurality of scanning systems," a "plurality of anti-virus servers," and a "plurality of switches," claim 1 of Application Serial No. 10/024,202 recites only a single one of each of these elements.

Whereas instant claim 8 is directed to a "method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising: directing incoming electronic mail from the internet backbone to a scanning system; scanning incoming electronic mail for malicious code; and downloading anti-virus code to clients coupled to the intranets," claim 1 of Application Serial No. 10/024,202 recites no such method.

Whereas instant claim 10 recites "at the one of the mail proxy servers, determining whether the incoming electronic mail is to be scanned for malicious code," claim 1 of Application Serial No. 10/024,202 recites no mail proxy servers at all.

The Examiner fails to indicate in the final rejection specifically why the subject matter of each of instant claims 1, 3, 5, 8, and 10, with the differences over claim 1 of Application Serial No. 10/024,202, as indicated supra, would have been obvious over claim 1 of Application Serial No. 10/024,202. Therefore, the Examiner has failed to present a prima facie case regarding the obviousness of the instant claimed subject matter.

The Examiner's rationale for the obviousness-type double patenting rejection, as it appears in the final rejection of August 15, 2006 reads, in toto, as follows:

> The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows: both applications claim a scanning system, an anti-virus server, and a switch for performing the same virus protection procedures. Although co-pending application discloses the scanning system notifies security manager upon detection of virus, one with ordinary skill in the art would understand that upon detection of virus, notification to administrator or security personnel is appropriate and required. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to notify security manager upon detection of virus.
>
> Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Merely because "both applications claim a scanning system, an anti-virus server, and a switch for performing the same virus protection procedures" is insufficient to establish obviousness-type double patenting because such reasoning does not take into account other, differing, features of the claims in each application. For example, the Examiner has not

addressed the "mail proxy server" of instant claim 3 and why this claim would have been obvious over claim 1 of the copending application.

The Examiner has touched on the "generating and transmitting an event indicating the detection to a security manager" of claim 1 of the copending application being different from instant claim 1 which does not require this limitation. But, all that the Examiner asserts is that the skilled artisan "would understand that upon detection of virus, notification to administrator or security personnel is appropriate and required." Appellants respectfully traverse the Examiner's reasoning. Contrary to the Examiner's apparent conclusion, there is no requirement that upon detection of a virus, an administrator or security personnel **must** be notified of such detection. A detection of a virus may just as well cause an elimination of that virus without ever notifying a security manager. In the absence of evidence to the contrary, and the Examiner has clearly proffered no such evidence, one cannot reasonably conclude that it would have been obvious, from a teaching of responsive to the detection of a malicious code, generating and transmitting an event indicating the detection to a security manager, to **not** generate and transmit such an event to a security manager, or vice versa. The Examiner must indicate some **reason** for concluding that it would have been obvious to eliminate "in response to detection of an instance of malicious code, generating and transmitting an event indicating the detection to a security manager" from claim 1 of the copending application, but the Examiner has merely set forth the conclusion that this would have been obvious rather than a cogent rationale for reaching that conclusion.

With regard to independent claims 3, 5, 8, and 10, the Examiner never even deals with the differences, pointed out supra, between these claims and claim 1 of the copending application.

Accordingly, since the Examiner has failed to establish a prima facie case of obviousness with regard to instant claims 1, 3, 5, 8, and 10, and because the instant claimed subject matter is

patentably distinct over claim 1 of co-pending application 10/024,202, the rejection of these claims under obviousness-type double patenting must be reversed.

B. CLAIMS 1, 3, 5, 8, AND 10 ARE NOT RENDERED OBVIOUS BY *BATES ET AL.*

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision always rests upon the Examiner. *In re Mayne*, 104 F.3d 1339, 41 USPQ2d 1451 (Fed .Cir. 1997); *In re Deuel*, 51 F.3d 1552, 34 USPQ2d 1210 (Fed. Cir. 1995); *In re Bell*, 991 F.2d 781, 26 USPQ2d 1529 (Fed. Cir. 1993); *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner is required to provide a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 357 F.2d 385, 148 USPQ 721 (CCPA 1966); *In re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970).

Each of independent claims 1, 3, and 5 requires a "switch" or a "plurality of switches" that must be "coupled between the internet backbone, the scanning system(s), and the anti-virus server(s)." The switch, or switches, is/are "configured for: directing incoming electronic mail" either from the internet backbone to the scanning system or from the internet backbone to the mail proxy server, or to at least one of the scanning systems. Claims 8 and 10, while not directly reciting a "switch," per se, still require "directing incoming electronic mail from the internet backbone" to either a scanning system or to one of a plurality of mail proxy servers.

The Examiner relies on Figure 3 of *Bates et al.* for the claimed "switch," finding that "the web server allows different security applications," and on col. 7, line 66 –col. 8, lines 11 of *Bates et al.* for the claimed configuration of the switch, finding that "the data are re-directed to the server for checking" (Final Rejection of August 15, 2006-page 4).

Appellants are unable to find any "switch," as claimed, in *Bates et al.* To the extent that the Examiner relies on Figure 3 of *Bates et al.*, no switch is depicted therein. To the extent the Examiner relies on a web server that allows different security applications, this is no indication of any type of "switch," particularly in the sense claimed, wherein the "switch" must be coupled between the internet backbone, the scanning system, and the anti-virus server. Merely because a web server may allow different security applications, this is no specific teaching or suggestion of "switching" between such applications, let alone a "switch" that is coupled between the internet backbone, the scanning system, and the anti-virus server, as claimed.

With regard to the specific claimed configuration of the switch, i.e., for directing incoming electronic mail from the internet backbone to the scanning system or to the mail proxy server, the Examiner's reliance on data being re-directed to a server for checking does not teach or suggest this very specific claim limitation. Specifically, the Examiner relies on col. 7, line 66-col. 8, line 11 of *Bates et al.* for the claimed switch configuration. That portion of *Bates et al.* reads as follows (Emphasis Added):

> Referring now to FIG. 4, a method 400 in accordance with the preferred embodiments allows a virus checker on **a web server to automatically check e-mail messages, web pages, and downloaded files for viruses before passing these on to a web client.** Method 400 begins when a web client requests **information that normally would flow through the web server to the web client** (step 410). If the request does not require virus checking (step 420=NO), the requested information is sent to the web client (step 480). If the request requires virus checking (step 420=YES), a virus check is performed on the requested information (step 430). If no virus is found (step 440=NO), the requested information is sent to the web client (step 480).

Thus, *Bates et al.* make it clear that information **normally flows** through the web server to the web client and the web server performs the virus checking procedure on e-mail messages, web pages, and downloaded files before they are sent to the client. All information requested by the client, then, **normally** flows through the web server to be checked for viruses and is not

"redirected to the server for checking," as asserted by the Examiner. There is no capability or motivation by *Bates et al.* to employ a switch to direct different types of traffic to different types of servers before being sent to the clients. In *Bates et al.*, **all traffic that is to be sent over to the clients normally go through a single web server without being directed by a component such as a switch**, much less "a switch coupled between the internet backbone, the scanning system and the anti-virus server." *Bates et al.* merely distinguish between the different types of traffic **arriving** at the web server and accordingly performs virus checking in the web server. Also, there is no disclosure of directing the different types of traffic to specific servers, such as "directing incoming electronic mail from the internet backbone" to either a scanning system or to one of a plurality of mail proxy servers, as claimed.

C. CLAIMS 2, 4, 6, 7, 9 AND 11-15 ARE NOT RENDERED OBVIOUS BY *BATES ET AL.* IN COMBINATION WITH ANY OF THE OTHER APPLIED REFERENCES

Moreover, the addition of the *Caccavale*, *Kim et al.*, and/or *NAI* references does nothing to provide for the deficiencies of *Bates et al.* noted supra. Therefore, the obviousness rejections of dependent claims 2, 4, 6, 7, 9, and 11-15 must also be reversed.

More particularly, with regard to claims 2, 4, 7, and 9, since there is no "switch," as claimed, in *Bates et al.*, regardless of any "decoy server" of *NAI*, the combination of references would still lack a switch, especially a switch that "is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server."

Similarly, with regard to dependent claims 6 and 11, since there is no "switch," as claimed, in *Bates et al.*, regardless of any "load balancing" suggested by *Caccavale*, the

combination of references would still lack a switch, especially a switch that is further configured for "load balancing" among scanning systems and among the decoy servers, or among the mail proxy servers.

With regard to dependent claims 12-15, since there is no "switch," as claimed, in *Bates et al.*, regardless of anything taught or suggested by *Kim et al*, relative to a hub and sanitizing electronic mail, the combination of references would still lack the claimed "switch" in combination with a hub in communication with the scanning system and the intranets and a sanitizing of at least some of the incoming electronic mail addressed to recipients on the intranets.

VIII. CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, Appellants request the Honorable Board to reverse each of the Examiner's rejections.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

3/16/07
Date

Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9952
Fax. 703-519-9958

IX. CLAIMS APPENDIX

1. (Original) A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;

an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and

a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:

directing incoming electronic mail from the internet backbone to the scanning system.

2. (Original) A network security system according to claim 1, further comprising:

a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;

wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

3. (Original) A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;

a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code and directing the incoming electronic mail to the scanning system when the incoming electronic mail is determined to be scanned for malicious code;

an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and

a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:

directing incoming electronic mail from the internet backbone to the mail proxy server.

4. (Original) A network security system according to claim 3, further comprising:

a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;

wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

5. (Original) A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code;

a plurality of anti-virus servers coupled to the intranets for downloading anti-virus code to clients coupled to the intranets;

a plurality of switches coupled between the internet backbone, the scanning systems, and the anti-virus servers, said switches configured for:

directing incoming electronic mail to at least one of the scanning systems.

6. (Original) A network security system according to claim 5, wherein the switches are further configured for:

load-balancing among the scanning systems and among the decoy servers.

7. (Original) A network security system according to claim 5, further comprising:

a plurality of decoy servers coupled to the intranets for masquerading as legitimate servers and logging activity on communications received via the internet backbone;

wherein the switches are further coupled to the decoy servers and are further configured for redirecting suspicious traffic from the internet backbone to the decoy servers.

8. (Original) A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to a scanning system;

scanning incoming electronic mail for malicious code; and

downloading anti-virus code to clients coupled to the intranets.

9. (Original) A method according to claim 8, further comprising:

redirecting suspicious traffic from the internet backbone to the decoy server;

simulating the decoy server as a legitimate server to the suspicious traffic; and

logging activity on communications received via the internet backbone.

10. (Original) A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to one of a plurality of mail proxy servers;

at the one of the mail proxy servers, determining whether the incoming electronic mail is to be scanned for malicious code and directing the incoming electronic mail to a scanning system when the incoming electronic mail is determined to be scanned for malicious code;

at the scanning system, scanning incoming electronic mail for malicious code;

downloading anti-virus code to clients coupled to the intranets.

11. (Original) A method according to claim 10, further comprising:

load-balancing among the mail proxy servers.

12. (Original) A network security system according to claim 1, further comprising:

a hub in communication with the scanning system and the intranets, wherein the scanning system is further configured for sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets and directing the sanitized incoming electronic mail to the recipients via the hub.

13. (Original) A network security system according to claim 3, further comprising:

a hub in communication with the scanning system and the intranets, wherein the scanning system is further configured for sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets and directing the sanitized incoming electronic mail to the recipients via the hub.

14. (Original) A method according to claim 8, further comprising:

sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets; and

directing the sanitized incoming electronic mail to the recipients on the intranets.

15. (Original) A method according to claim 10, further comprising performing, at the scanning system, the steps of:

sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets; and

directing the sanitized incoming electronic mail to the recipients on the intranets via a hub in communication with the scanning system and the intranets.

X. EVIDENCE APPENDIX

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI. RELATED PROCEEDINGS APPENDIX

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.